UNIVERSIDAD AUTONOMA DE MADRID

ESCUELA POLITECNICA SUPERIOR

Grado en Ingeniería Informática

TRABAJO FIN DE GRADO

DESARROLLO DE PORTALES CAUTIVOS WIFI E IMPLICACIONES EN SEGURIDAD

Pedro Almendral Fernández
Tutor: Javier Aracil Rico

JULIO 2020

DESARROLLO DE PORTALES CAUTIVOS WIFI E IMPLICACIONES EN SEGURIDAD

AUTOR: Pedro Almendral Fernández
TUTOR: Javier Aracil Rico

Dpto. de Ingeniería Informática
Escuela Politécnica Superior
Universidad Autónoma de Madrid
Julio de 2020

Resumen (castellano)

Este proyecto trata esencialmente de un trabajo de concienciación sobre ciberseguridad, más concretamente centrado en el dominio relativo a las redes wifi públicas.

Inicialmente se justifican los motivos y factores de decisión para la realización del proyecto, plasmando los objetivos que se desean alcanzar y proporcionando una puesta en contexto de la situación actual y del interés que esta representa, mediante las principales ideas a desarrollar, tomando como referencia los acontecimientos sucedidos a lo largo de los últimos años, pasando por unos determinados tipos de amenazas así como por las acciones llevadas a cabo por grupos criminales y los trabajos realizados al respecto por autoridades en el sector de la seguridad.

Una vez establecidas estas bases y teniendo clara la idea de la importancia de la protección de nuestros datos, se presenta el proyecto a desarrollar, consistente principalmente en la creación de una red wifi falsa en conjunto con una página web que, actuando como un portal cautivo, solicita autenticación a través de credenciales de varios servicios con la intención de adueñarse de ellas. Más detalladamente se mostrará el diseño completo de la aplicación, especificando la necesidad y la utilidad de cada uno de los elementos individuales que forman parte de ella.

A continuación, se entrará en el desarrollo práctico, mostrando y explicando los pasos que se han llevado a cabo para lograr cumplir con esta propuesta.

Finalmente se exponen las pruebas realizadas a nivel individual y de integración de todo el proyecto, mostrando los resultados obtenidos y las conclusiones extraídas, aprovechando las mismas para finalizar dando una serie de consejos, soluciones y buenos hábitos de utilidad para evitar vernos inmersos en situaciones no deseadas y ser capaz de defendernos de los peligros que acechan en internet.

Abstract (English)

This Bachelor Thesis is about raise awareness regarding cybersecurity, specially focusing at public wifi networks.

To start with, the decisive factors for the elaboration of this project are justified, reflecting the objectives to be achieved and putting into context the current situation and the interest that it represents by the main ideas, taking as reference some of the events that took place during the last years, going through different threats as well as the criminal groups actions and the labor done by authorities in relation to the security sector.

Once this bases are established and having clear the idea of the protection of our data, the project is presented, which mainly consist in the creación of a fake wifi network together with a web page that works as a captive portal, asking for the users credentials with the purpose of taking control of them. The application design will be shown in more detail, specifying the need and utility of each single element of it.

Then we will see the practice development, showing and explaining the steps followed to achieve this proposal.

Finllay, the performed individual and global tests are exposed, displaying the results obtained from them and making using of that to give a series of tips, solutions and good habits of utility to avoid getting involved in unwanted situations and being able to defend ourselves from the internet hazards.

Palabras clave (castellano)

SSID, APT, Malware, DarkHotel, Phising, Raspberry, Troyano, Gusano, Ransomware, Botnet, VPN.

Keywords (inglés)

SSID, APT, Malware, DarkHotel, Phising, Raspberry, Troyano, Gusano, Ransomware, Botnet, VPN.

Agradecimientos

A mis profesores por todo lo que me han enseñado y que me ha permitido legar hasta aquí.

A toda mi familia y mis amigos por su preocupación, su apoyo incondicional y por estar siempre en los momentos difíciles.

INDICE DE CONTENIDOS

INDICE DE FIGURAS

1 Introducción

1.1 Motivación

Hace ya unos años entramos en la era de la información, y con el tiempo y la alta velocidad de desarrollo de la informática, ésta se ha vuelto parte de nuestras vidas inevitablemente.
Vivimos conectados al resto del mundo mediante internet de una u otra manera, actualmente, ¿quién no tiene un dispositivo con acceso a internet? Podríamos decir que es algo esencial y todos los utilizamos cuando interactuamos mediante las redes sociales, hablamos con alguien a través de una aplicación o navegamos por la web para realizar compras o simplemente buscar información.
Esto es una realidad, y desde luego ha traído un montón de progresos y herramientas de utilidad al mundo; tenemos acceso a cualquier cosa que necesitemos saber de una manera inmediata, fuentes de entretenimiento ilimitado, comunicación con todo el mundo en cualquier momento y en cualquier lugar y en general grandes facilidades en una multitud de aspectos de la vida.
Sin embargo, el aumento de esta actividad ha puesto en riesgo prácticamente la totalidad de nuestra información, incluso la más sensible, sin que nos hayamos siquiera dado cuenta, y ahora está expuesta al mundo y al alcance de muchas personas que, si quieren molestarse en obtenerla, pueden conseguirlo de una manera no demasiado complicada.
Simplemente desde una cafetería, un restaurante, una sala de espera o cualquier lugar público podrían estar robando nuestra información sin que nos diésemos cuenta.
La mayoría de la gente no es consciente de que esto ocurre, y aunque lo sea, muchas veces pesa más el hecho de conseguir esa preciada conexión wifi para poder hacer al instante montones de cosas que realmente no son tan esenciales como creemos.
Nuestra privacidad está en juego y es muy importante, en un principio podría no parecer algo tan peligroso, pero imaginemos por un momento que alguien tuviera acceso a toda nuestra actividad en internet, y sobre todo, que tuviera la capacidad de usarla a su antojo, sería realmente preocupante, por ello es de gran valor la concienciación de las personas respecto a este tema, y este trabajo pretende hacer entender su importancia demostrando las vulnerabilidades existentes y proponiendo soluciones a ellas.

1.2 Objetivos

Con este proyecto se pretende alcanzar una serie de objetivos relacionados con diversos aspectos.
En primer lugar, **dar a conocer la importancia de la seguridad de la información** en la actualidad de una manera general y más específicamente en lo relativo a las redes públicas, haciendo énfasis en el incremento del interés que ésta adquirirá en el futuro.
Conseguir **concienciar** a las personas **del riesgo que supone perder el control sobre sus datos personales**, y la **facilidad con la que esto puede suceder**, exponiendo lo abierta que está nuestra privacidad a través de internet debido a las vulnerabilidades de los sistemas donde almacenamos nuestros datos y mostrando las mayores amenazas en el campo de la ciberseguridad wifi.
Para lograr esto, **aprender a identificar y distinguir los diferentes métodos de robo de información** mediante ataques muy habituales y de gran peligro que se usan hoy en día, así como las correspondientes **medidas de prevención y soluciones** ante ellos.

Por otra parte, se proponen **objetivos más concretos a nivel de desarrollo**, tales como **conocer el funcionamiento de los principales protocolos** de comunicación de internet, **familiarizarse con el uso de una Raspberry Pi** y la selección y el uso de determinadas herramientas software en conjunto para generar un punto de acceso wifi, **aprender a diseñar una página web** tanto desde un punto de vista estructural como estilístico y a **configurar y desarrollar un portal cautivo**, que es el elemento principal del proyecto.

1.3 Organización de la memoria

La memoria consta de los siguientes capítulos:

1. **Introducción.** En él se expone la motivación del proyecto y los objetivos que se pretenden alcanzar con él, que no son otros que conocer las posibles vulnerabilidades que pueden ser aprovechadas por ciberdelincuentes para cometer delitos.
2. **Estado del Arte.** En este capítulo se realiza un estudio acerca de la forma de lograr los objetivos expuestos, así como los distintos autores y métodos que utilizaron para conseguir objetivos similares, todo ello desde una perspectiva de hacking ético y educativo.
3. **Diseño.** Se expone en este apartado el esquema de trabajo a utilizar, así como las herramientas, tanto software como hardware, que serán necesarias para poder llevar a efecto el proyecto. Se ha elegido como hardware una solución de bajo costo y algo desfasada tecnológicamente (Raspberry Pi 3 B, la cual salió al mercado en 2016), para demostrar que no es necesario la utilización de potentes sistemas informáticos si se quiere engañar a una persona. Para el sistema operativo se ha elegido un entorno Linux (Debian), optimizado para la arquitectura de la Raspberry Pi 3 B, conocido como Raspbian.
4. **Desarrollo.** Se detalla la parte práctica del proyecto, la forma en que se ha llevado a cabo y la configuración de hardware y software.
5. **Integración, pruebas y resultados.** Una vez se ha configurado todo, llega el momento de mostrar el funcionamiento conjunto a través de pruebas reales y ver los resultados que se pueden obtener.
6. **Conclusiones y trabajo futuro.** Por último, se extraen las conclusiones finales de todo el proyecto, y que podrían resumirse en que no siempre es gratis todo lo que lo parece, si no que en ocasiones el precio a pagar puede ser muy alto.

Referencias. Aquí se incluye un listado de las fuentes de información utilizadas.
Glosarios. Es la sección de definición de las palabras clave utilizadas.

2 Estado del arte

Han sido diversos programas y artículos relacionados con la seguridad informática en el ámbito de las redes públicas los que me han llamado la atención y me han impulsado a realizar este proyecto.

Realmente hasta hace poco yo no me preocupaba demasiado de este este tema porque ni siquiera era muy consciente de lo que suponía, pero a la vista de todas las noticias al respecto y de la gran cantidad de personas que son víctimas de robos de información y posteriormente de extorsiones y estafas, es evidente que no es un problema para tomarse a la ligera.

Esta es una cuestión a la que se le ha dado voz, sin embargo, quizás no la suficiente, porque a pesar de todas las precauciones que se enseñan y todas las consecuencias que se advierten que pueden llegar a existir, aún hay mucha gente que sigue siendo atacada con éxito, principalmente usuarios nuevos en el mundillo de la informática o aquellos más casuales son los más propensos a caer en engaños, precisamente por este desconocimiento. Incluso personas más experimentadas no lo llegan a tomar en serio y siguen dándole demasiada importancia a un momentáneo acceso a internet a costa de poner en riesgo muchos de sus datos, hasta que pierden el control sobre ellos.

Actualmente una gran parte de la población (todos los que tenemos un dispositivo con conexión wifi) somos potenciales objetivos de algún algún ataque de este tipo, y aunque algunos determinados perfiles lo son más que otros, eso no le otorga inmunidad a nadie.

Es por ello por lo que en esta sección voy a realizar una puesta en contexto de la situación mediante la exposición y el análisis con apoyo de datos, de las posibles amenazas en este ámbito, así como de diversos tipos de noticias y acontecimientos, desde pequeña a gran escala, de importancia para este campo. También hablaré de alguna personalidad de relevancia para el mismo.

2.1 Visión general de las amenazas

El Instituto Nacional de Estadística[1] menciona lo siguiente en sus notas de prensa del 16 de octubre de 2019: “La mayoría de los internautas de los tres últimos meses (el 95,6%) ha utilizado algún tipo de dispositivo móvil para acceder a internet fuera de la vivienda habitual o el lugar de trabajo”

Y es que no son pocas las veces que hemos visto carteles como el de la Figura 2-1, ofreciéndonos una tentadora conexión a internet, pero al mismo tiempo, dando pie a los cibercriminales para cometer sus fechorías.

Figura 2-1: Cartel de zona wifi gratis en un local

De hecho, este es el escenario perfecto para ser víctima de un ataque, ya que por lo general estas zonas suelen ser bastante concurridas y hay grandes probabilidades de que alguien sin mucha precaución se conecte a una red que no sea la legítima.

Las redes wifi públicas suelen ser libres de contraseña, pero cuentan con un portal cautivo, que es una página de ingreso previa a conceder la conexión. En este tipo de páginas, como la de la Figura 2-2, se suele proporcionar una información básica acompañada de un formulario a rellenar por el usuario con ciertos datos de identificación, como pueden ser, habitualmente, un par usuario-contraseña registrado, un código de acceso o una cuenta de otro servicio como Google.

Existen redes wifi que ni siquiera solicitan este paso previo, lo cual es aún más peligroso, porque no se tiene un control sobre las conexiones, sin embargo, no es lo habitual, de hecho es un indicio de riesgo por poder tratarse de una red falsa.

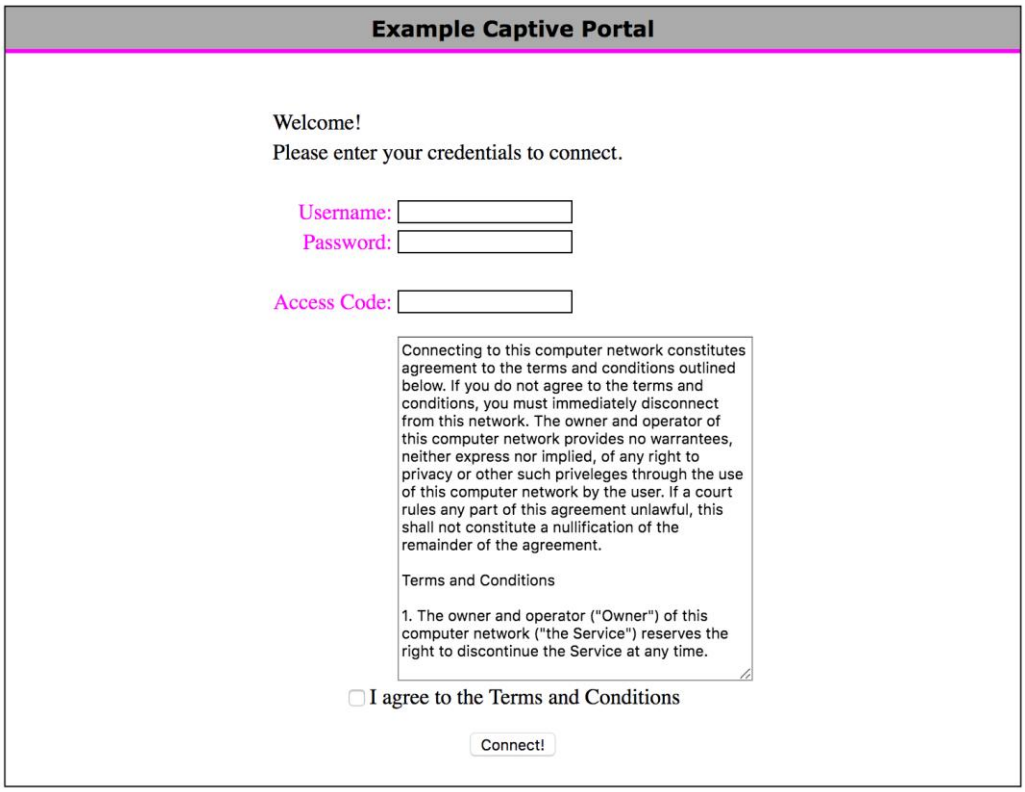

Figura 2-2: Portal Cautivo de una red wifi pública

En cualquiera de estos casos, al conectarnos a una red wifi que no conocemos sin total certeza de su fiabilidad, entramos en peligro de sufrir alguno de los ataques que vamos a ver a continuación.

2.1.1 Man-in-the-Middle

Supongamos que tenemos interés en averiguar algo importante que una persona quiere decirle a otra y necesitamos una manera de conseguirlo. Podemos pensar que una posibilidad sería pedir la información al emisor para hacer de intermediario entre él y el receptor, pero si la información es delicada, no vamos a conseguir ese permiso, con lo que deberemos engañar a esa persona para que crea estar hablando con quien quiere, por ejemplo, mediante un correo electrónico falso con el que nos haríamos pasar por el objetivo. En el ámbito de la ciberseguridad, esta es la idea de uno de los ataques más habituales, conocido como Man-in-the-Middle.

Este ataque consiste en la intrusión de un agente adicional en medio de una comunicación entre dos extremos, como se representa en la Figura 2-3. El intermediario adquiere así acceso a la información intercambiada, pudiendo leerla y modificarla a voluntad.

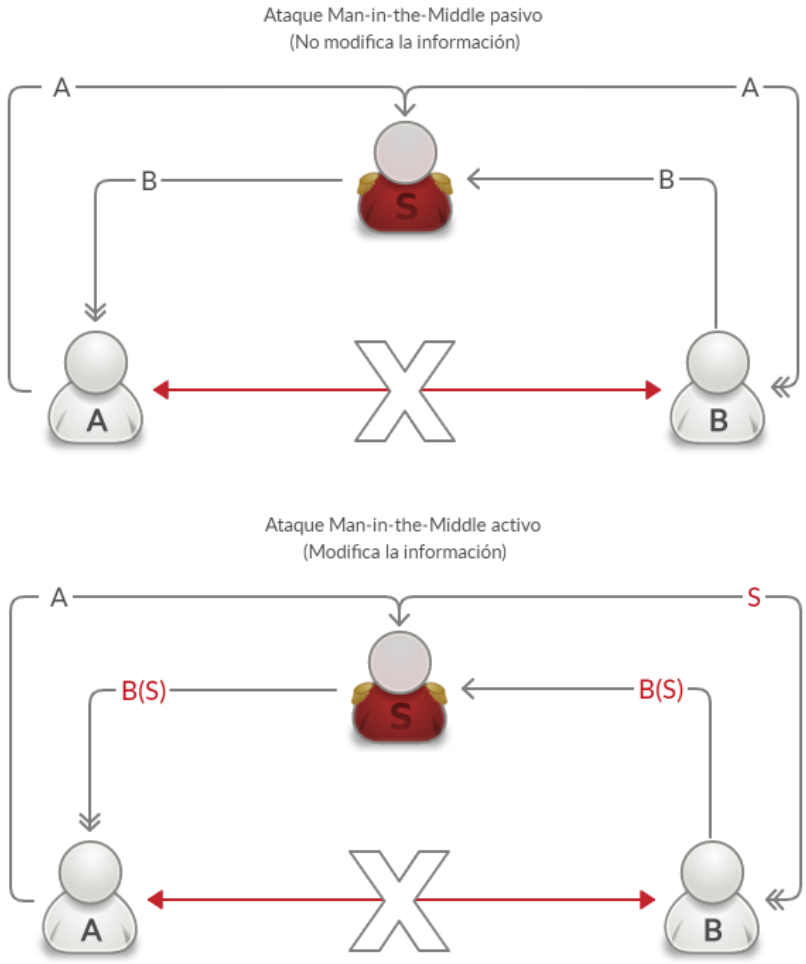

Figura 2-3: Esquema de un ataque Man-in-the-Middle

En el caso particular de las redes wifi públicas este es un ataque sencillo de realizar a la par que efectivo. Puesto que la conexión wifi es abierta, el atacante puede generar su propia red provocando que un usuario se conecte a ella por error, consiguiendo así ser un punto de paso de todas las peticiones que se realicen.

Con uno de los muchos softwares de análisis paquetes gratuitos que existen actualmente, como Wireshark, podríamos ver las tramas de red que contienen la información de los mensajes. De este modo, tendríamos acceso a todos los datos de la comunicación, mientras que estaríamos concediendo acceso real a internet a la víctima para que no sospechara nada. Se puede ver un ejemplo de esto en la Figura 2-4.

El principal inconveniente de este ataque es que si la información viaja cifrada no seríamos capaces de entenderla a pesar de conocerla. Afortunadamente para nosotros, muchas redes wifi no proporcionan cifrado, sin embargo, muchas webs conocidas sí que lo llevan en la capa de transporte a cabo a través del uso del protocolo HTTPS, por lo que cada vez es más difícil obtener información clara de este modo.

Del mismo modo también existen métodos para lograr deshacer el cifrado de los datos, pero el ataque se vuelve notablemente más complejo.

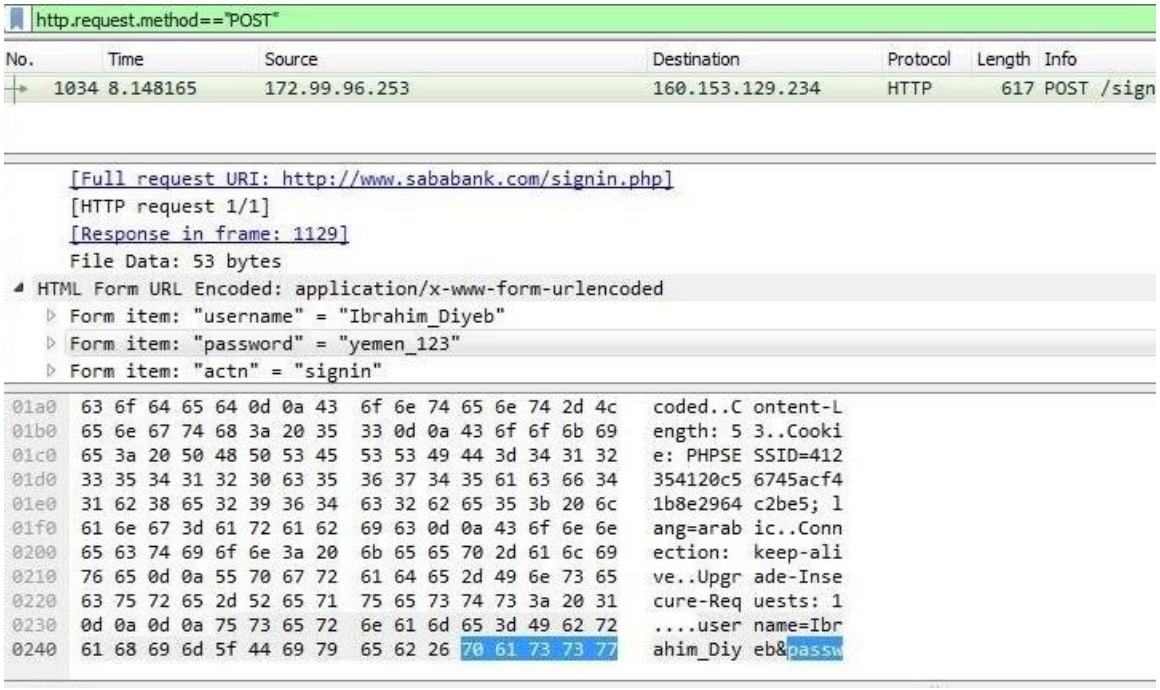

Figura 2.4: Paquete en texto claro a través de Wireshark

2.1.2 Suplantación de DNS

Este ataque, también conocido como envenenamiento de DNS (representado en la Figura 2-5) trata de reemplazar el servidor de nombres de dominio del usuario, por otro malicioso configurado por el propio atacante, donde sustituye la dirección IP asociada a un determinado nombre de un servidor por otra que dirige al usuario hacia una web fraudulenta en la que el atacante tiene el control y desde donde puede tratar de infectar el equipo de la víctima.

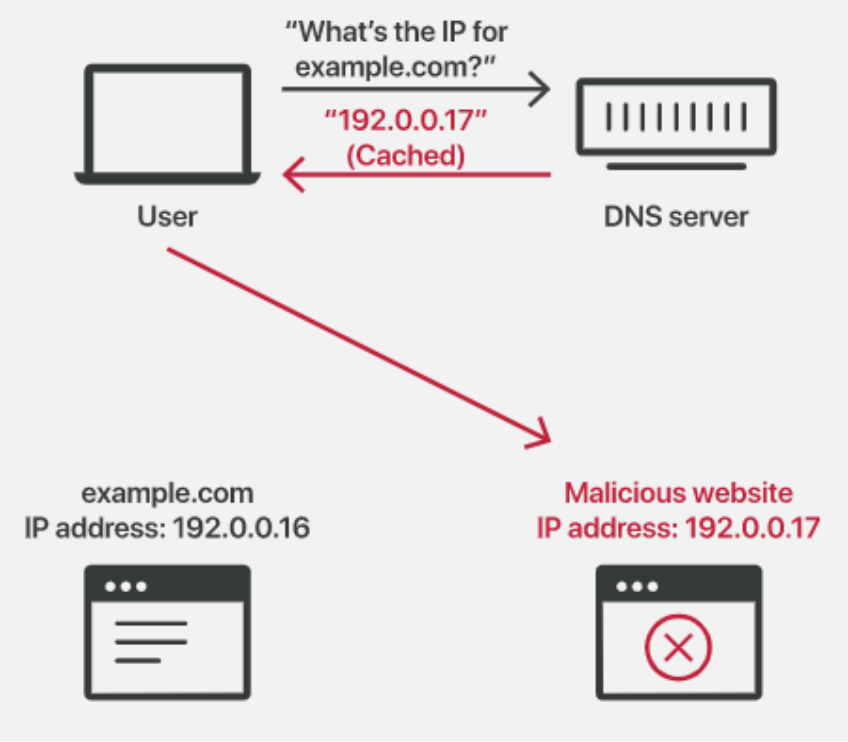

Figura 2-5: Esquema de un ataque de envenenamiento de DNS.

Este ataque se puede llevar a cabo después de haberse infiltrado en la comunicación mediante un Man-in-the-Middle.

2.1.3 Ataques derivados

Los ataques anteriores, aparte de ser habituales, no demasiado complejos de realizar, bastante exitosos y ya peligrosos en sí mismos, pueden derivar en otro tipo de amenazas y desencadenar un mal mucho mayor.

Ambos comparten el mismo objetivo robar información personal, tal como credenciales de diversos sitios, datos bancarios u otro tipo de información privada detallada.

Con estos datos los atacantes adquieren mucho poder, teniendo la capacidad apropiarse de cuentas de correo, redes sociales, así como otros perfiles de interés, de realizar transacciones financieras a su favor, de sacar beneficio directo mediante la extorsión con los datos recopilados, e incluso de suplantar la identidad de la víctima para todo tipo de fines, pudiendo llegar a continuar cometiendo crímenes bajo su nombre.

Todo este tipo de acciones se pueden alcanzar mediante la infección del equipo de la víctima con algún tipo de malware, como puede ser un troyano para abrirse un acceso al mismo, un gusano para propagar la amenaza, un ransomware que limite o bloquee totalmente su funcionalidad o convertirlo en parte de un botnet, por mencionar algunos de los términos más conocidos.

2.2 Acontecimientos a gran escala

2.2.1 DarkHotel

DarkHotel[2] es el nombre de una campaña de espionaje cuyos primeros indicios se remontan al año 2007, aunque las primeras señales de ataques datan de inicios del año 2009.

Esta campaña ha tenido muchos años de recorrido y aún sigue activa en la actualidad. El principal objetivo de sus integrantes es realizar ataques a través de la red wifi en hoteles de lujo, principalmente asiáticos, tomando como objetivo a altos cargos ejecutivos para conseguir acceso a sus equipos y de ese modo a información privilegiada que luego pueden utilizar de diversas maneras para obtener beneficio.

Las personas que se conectan a una wifi afectada bajo su control corren el riesgo de ser infectadas mediante correos electrónicos que contiene algún tipo de malware aprovechando vulnerabilidades del día cero para falsificar actualizaciones de software bien conocido como por ejemplo Adobe Flash. Esta estrategia de ataque se refleja bien en la Figura 2-6.

Destacan entre las capacidades de este grupo el uso de botnets para controlar toda la red, los certificados digitales ilegítimos o el malware especializado que se encarga de robar los datos.

Los ataques realizados por este grupo han sido clasificados por la compañía internacional de ciberseguridad Kaspersky como APT (Advanced Persistent Threat), es decir que son un tipo de amenaza muy duradera en el tiempo.

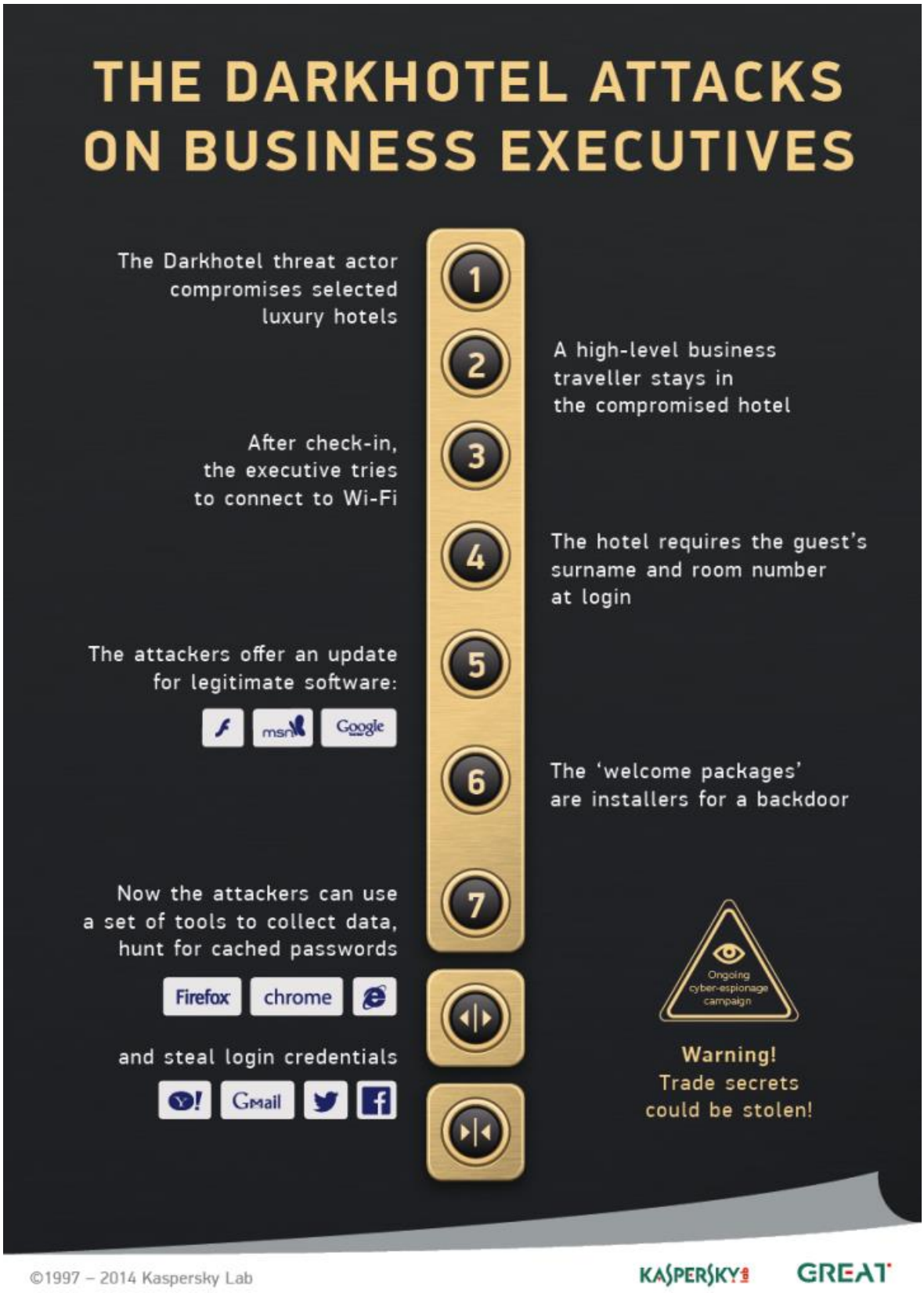

Figura 2-6: Ataques DarkHotel

2.2.2 Magecart Group 5

En este último año 2019 ha salido a la luz un nuevo proyecto de cibercrimen del conocido como “Magecart Group 5”.
Su objetivo era exponer routers de redes públicas para robar la información de los usuarios y para ello utilizaron un método más sofisticado que los mencionados anteriormente, consistente en insertar un fragmento de código JavaScript malicioso en los archivos del router. En la Figura 2-7 se muestra un esquema con el procedimiento detallado.
El hecho de ser un grupo organizado supone una amenaza mucho mayor para los usuarios, ya no solo por sus conocimientos que les permiten elaborar ataques más potentes, si no por el alcance que estos pueden llegar a tomar.

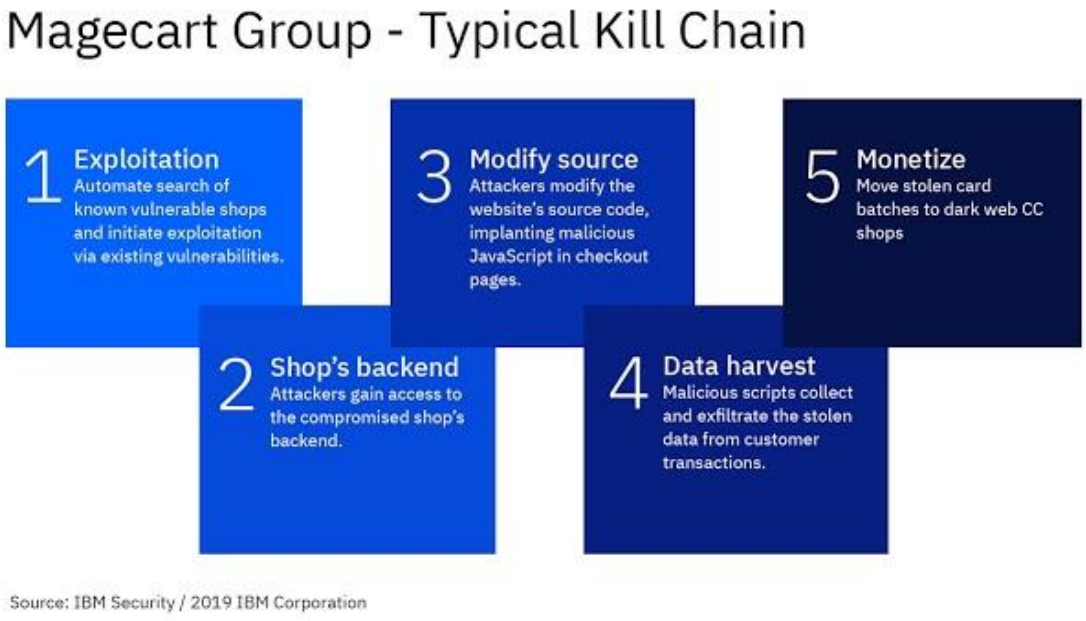

Figura 2-7: Metodología del grupo Magecart

2.3 Demostraciones

Ahora vamos a ver algunos ejemplos de personas que han conseguido demostrar que no hay que ser un experto en ciberseguridad para poder aprovecharse de las redes wifi públicas.

2.3.1 Betsy Davies

En el año 2015, la empresa proveedora de VPN "HideMyAss!" llevó a cabo un proyecto de concienciación protagonizado por Betsy Davies[3], una niña de 7 años de edad que, con el consentimiento de un experto pero sin ningún tipo de ayuda más que la información ofrecida por la propia internet, consiguió entrar en un ordenador de un cliente de una cafetería en menos de once minutos.
La manera en que lo hizo fue aprendiendo los pasos a realizar de un simple vídeo tutorial de YouTube, para a continuación realizar un ataque Man-in-the-Middle y recibir toda la información que la víctima transmitía.
Esto demuestra que no hay que tener unos conocimientos muy avanzados ni unos grandes recursos para dedicarse a ir robando datos a la gente, cualquier persona que se lo plantee puede hacerlo.

2.3.2 Chema Alonso

Chema Alonso es un prestigioso hacker español que ha divulgado sus conocimientos sobre seguridad informática en multitud de cursos y conferencias.
En 2013 realizó un experimento en el aeropuerto de Barajas de Madrid para un programa del canal "La Sexta"[4], en el que demostraba lo sencillo y accesible que es espiar a toda la gente que te rodea en un entorno con conexión wifi.
Durante el programa, Chema Alonso consigue acceso a la cuenta de correo de la víctima, a su perfil de Facebook, a sus contraseñas, e incluso, llega a infectar un teléfono móvil, tomando el control sobre los archivos multimedia de la víctima, sus conversaciones privadas, su ubicación y en definitiva, toda su vida digital.
Chema Alonso califica a las personas que realizan este tipo de actos como cibercriminales o piratas informáticos, que, al contrario que un hacker, no utilizan sus conocimientos para la investigación y el progreso de la seguridad, sino para todo lo contrario, para destruirla.

2.3.3 Wouter Slotboom

El caso de Wouter Slotboom es muy similar a los anteriores. Este experto en ciberseguridad afirma lo siguiente: "Solo necesitas 70 euros, un coeficiente intelectual medio y un poco de paciencia para espiar un dispositivo".
Él también realizó un ataque Man-in-the-Middle para situarse en medio de una red y en veinte minutos consiguió recabar una enorme cantidad de datos de un gran número de personas en una cafetería, obteniendo sus usuarios y contraseñas, datos de sus teléfonos móviles y muy valiosa información sin demasiado esfuerzo.

3 Diseño

3.1 Introducción

El trabajo a desarrollar va a consistir en la elaboración de una infraestructura con un conjunto de agentes cuya función se explicará a continuación.
Como elemento principal se desarrollará un portal cautivo, que con el apoyo de una red wifi falsa y un mecanismo de autenticación, pretende engañar a los usuarios para obtener sus credenciales.

3.2 Arquitectura

En esta sección se provee una visión general del sistema con todos sus componentes y la interacción entre ellos, así como el flujo de información desde el inicio hasta el final. La Figura 3.1 muestra un esquema de esta.

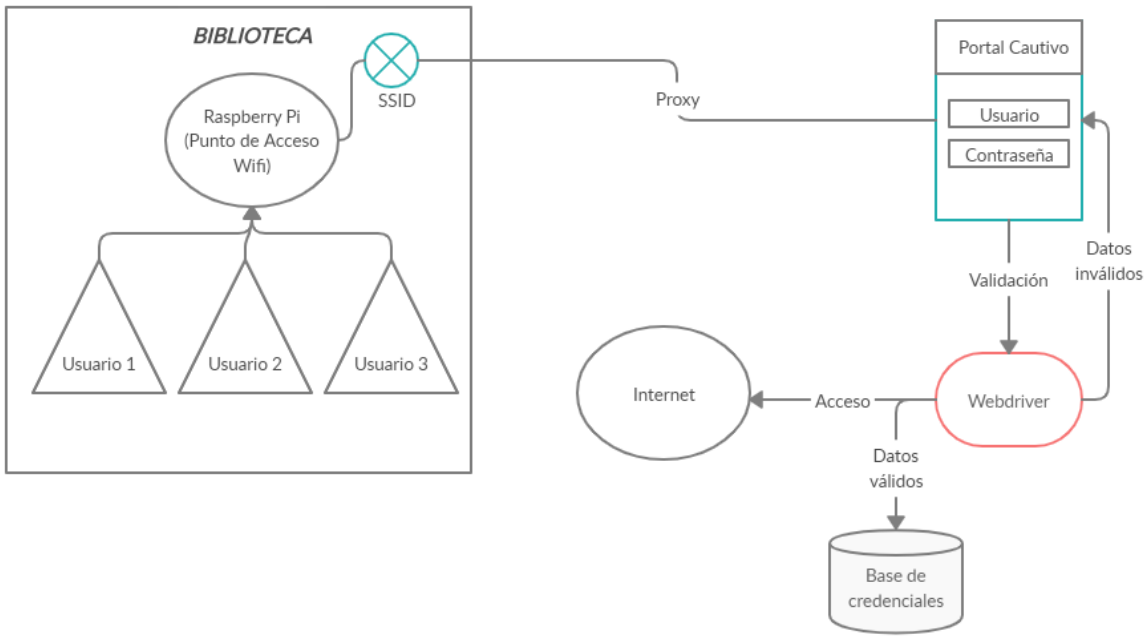

Figura 3.1: Esquema general.

El proceso comienza en un establecimiento público con acceso a internet, como podría ser una biblioteca. En este lugar se utilizaría una Raspberry Pi configurada como punto de acceso para conectarnos a la red wifi del local, de este modo estamos proporcionando una nueva red con un nuevo SSID que se aprovecha de la conexión a internet ya proporcionada. Esta red debe ser libre de contraseña para que todo el mundo pueda acceder a ella.
Con esto estaríamos provocando que los usuarios se conecten por error a esta red que acabamos de crear utilizando un SSID similar a la original y sobre la que tenemos control.
Cuando los usuarios intenten conectar a la red wifi mediante nuestro punto de acceso un servidor proxy los redirigirá a una página web local que previamente hemos diseñado y

que actuará como portal cautivo para solicitar registro antes de proporcionar acceso a internet.
En este punto será necesario que el usuario introduzca sus datos de la cuenta que nosotros deseemos para poder continuar. Los datos introducidos serán validados mediante un webdriver y sólo en caso de que sean correctos se le permitirá pasar el portal y acceder a internet, con el previo almacenamiento de sus credenciales ya verificadas.

3.3 Capas de la Web

La comunicación a través de internet está dividida en varias capas independientes entre sí, que encapsulan un conjunto de procedimientos simples regidos por una serie de protocolos, los cuales veremos en la siguiente sección.
Cada capa realiza una función determinada que comunica a la siguiente.
Esto es así porque desde un punto de vista global resultaría muy complicado, además de difícil de modificar.
A continuación,veremos estas capas en las que está dividida la estructura de la red.

3.3.1 Aplicación

La capa de aplicación es la más externa de todas, y la cual proporciona una manera de comunicarse con las inferiores, así como una serie de protocolos para enviar y recibir correos electrónicos (POP y SMTP), transferir archivos (FTP) y otras funciones. Los protocolos que nos interesan en este caso son DNS, DHCP, HTTP y su versión segura HTTPS.

3.3.2 Transporte

La capa de transporte es la que se encarga de establecer la comunicación punto a punto entre los sistemas involucrados y controlar la transferencia de la información.
Existen dos protocolos en esta capa, TCP, orientado a conexión, y UDP, no orientado a conexión. Hablaremos de ellos más adelante.

3.3.3 Red

La capa de red es la encargada de trasladar el paquete desde una máquina hasta otra, seleccionando la ruta más adecuada y dirigiéndolo desde el inicio hasta el final. La capa de red cuenta con un único protocolo, el protocolo IP, por lo que todas las máquinas deben implementarlo para tener acceso a la comunicación a través de internet.

3.3.4 Enlace

La capa de enlace dirige una trama entre dos routers contiguos, repitiéndose este paso entre todos los pares de routers que existen entre el origen y el destino. La capa de red establece cuales son los routers a seguir, mientras que la de enlace lleva a cabo esos pasos individualmente. Durante el trayecto pueden ser utilizados varios tipos de protocolos en cada enlace.

3.3.5 Física

La capa física lleva a cabo el transporte a más bajo nivel, es decir, traslada la información a nivel de bit mientras que las capas superiores trabajan con bloques de datos.

3.4 Protocolos

En esta sección vamos a ver todos los protocolos presentes en este proceso.

3.4.1 HTTP

El protocolo HTTP (Hypertext Transfer Protocol) es el protocolo de la capa de aplicación utilizado para transferir información a través de la web.
Este protocolo define una serie de mensajes que son mediante los cuales se lleva a cabo la comunicación entre un cliente y un servidor. El cliente envía un mensaje HTTP y el servidor le responde con otro que lleva el contenido solicitado.

Las páginas web están formadas por diversos archivos, un archivo HTML principal junto con otros referenciados como pueden ser otros archivos HTML, imágenes, ficheros de estilo CSS u otro tipo de archivos mediante su URL.

3.4.2 TCP/IP

TCP/IP (Transmission Control Protocol e Internet Protocol) son dos protocolos pertenecientes a las capas de transporte y de red respectivamente. Son los dos protocolos más utilizados y forman un grupo junto a muchos otros que aquí se mencionan como DNS o DHCP.

3.4.3 DNS

El sistema de nombres de dominio (DNS) es un mecanismo que establece una relación entre nombres de dominios web, que son los utilizados para ser más fácilmente reconocibles y sus respectivas direcciones IP, que son la manera práctica de identificar dónde se encuentran estos.

3.4.4 DHCP

DHCP o Protocolo de Configuración Dinámica de Host es un protocolo ejecutado generalmente en los routers y encargado de asignar direcciones IP a los equipos que se conectan a una red.

3.5 Herramientas utilizadas

En este apartado se exponen las herramientas utilizadas en el desarrollo del trabajo, las cuales, como quizás se pueda intuir, no son nada fuera de lo normal ya que no existe una exigencia muy elevada de recursos y hay mucho software gratuito a disponibilidad de todo el mundo. Estas son las siguientes:

- **Raspberry Pi**: Es el principal elemento ya que se trata del ordenador con el que se pondrá en funcionamiento la red wifi.
  Las Raspberry Pi son una familia de ordenadores de capacidades reducidas formados por una pequeña placa base, por este motivo generalmente son mucho más baratas en comparación a un ordenador portátil o de sobremesa, oscilando los precios alrededor de 40€.

El modelo aquí utilizado es una Raspberry Pi 3 B (Figura 3-2), que cuenta con puertos USB para conectar ratón y teclado, una conexión Ethernet, un módulo wifi integrado y una salida HDMI para el monitor. Es posible utilizar un modelo anterior siempre que cuente con estos componentes o se utilice un adaptador wifi externo.

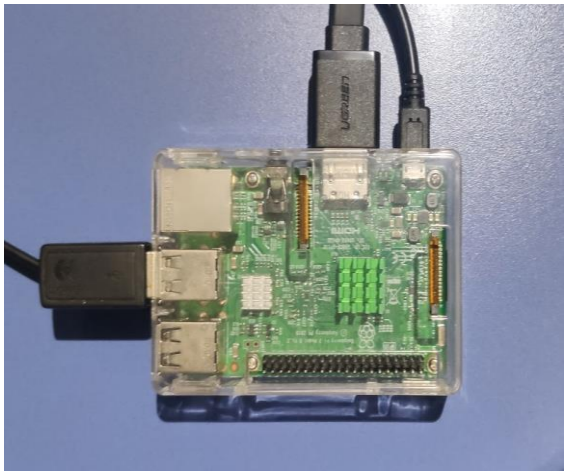

Figura 3-2: Raspberry Pi 3 Modelo B

La elección de este tipo de ordenador es debida a varios motivos. En primer lugar, su autosuficiencia para la función que se requiere, adicionalmente por su tamaño ya que es fácil tanto de transportar como de ocultar, características interesantes al querer utilizarlo en lugares públicos sin llamar demasiado la atención y por último, debido a su precio no supondría una gran pérdida en caso de requerir ser destruido durante una emergencia.

- **Software instalado:** Estos son los componentes adicionales que se han utilizado sobre la Raspberry Pi para dotarla del funcionamiento deseado:

    - **Sistema operativo**: La familia Raspberry cuenta con su propio grupo de sistemas operativos optimizados basados en Debian conocidos como "Raspbian" o "Raspberry Pi OS".
      Raspberry también admite sistemas Windows o Linux, pero la opción recomendada y la que se ha utilizado es la indicada en la página página oficial, llamada "Raspbian Buster".

    - **LAMP**: Es un conjunto de aplicaciones software que permiten alojar y gestionar un servidor web, su nombre procede de las siguientes aplicaciones, que son el sistema operativo Linux, el servidor web Apache, el gestor de base de datos MySQL/MariaDB y el lenguaje de programación del servidor que opera con los datos, PHP, todas ellas de código abierto.

    - **Visual Studio Code**: Editor de código con funciones de autocompletado, depuración, control de versiones Git y muchas otras herramientas. Utilizado para realizar el diseño de la web y generar el código del servidor.

    - **Consola de comandos**: Se trata de una función integrada en el sistema operativo que permite instalar, eliminar y actualizar paquetes, editar ficheros del sistema, navegar rápidamente por los directorios y operaciones

de todo tipo. A través de ella se instalan las herramientas de LAMP y se llevan a cabo las configuraciones.

- **Hostapd y dnsmaq**: Estos son dos paquetes que proporcionan los servicios necesarios para que el adaptador de red funcione como punto de acceso (hostapd) y los protocolos DHCP y DNS (dnsmasq).

- **Webdriver**: Controlador que facilita la realización de pruebas en la web. Proporciona funciones que simulan la interacción humana con a través del navegador, cómo seleccionar elementos, escribir texto, abrir ventanas o comprobar valores, entre otras utilidades. El webdriver utilizado es ChromeDriver, la versión para Google Chorme, pero también existen otros con las mismas funciones para otros navegadores, como geckodriver en Mozilla Firefox. Es necesario para automatizar el proceso de comprobación de los datos durante el inicio de sesión en la página web.

- **Nodogsplash**: Es el software de portal cautivo, un elemento fundamental que proporciona la funcionalidad de presentar la página web deseada al solicitar conexión con la red wifi y habilita el acceso a internet una vez comprobadas las credenciales de inicio de sesión.

4 Desarrollo

4.1 Instalación y configuración

Este proyecto ha sido realizado en una Raspberry Pi 3 Modelo B Versión 1.2 con el sistema operativo instalado Raspbian Buster, los pasos a seguir pueden no ser exactamente igual si se utiliza otro modelo de Raspberry o un sistema operativo diferente del mencionado.

1. Instalación del sistema operativo y configuración inicial:

La imagen de Raspbian Buster puede descargarse desde la página de la "Raspberry Pi Foundation" (https://www.raspberrypi.org/downloads/raspbian/)

Necesitaremos una tarjeta microSD y un software de flasheo, como Etcher, para grabar la imagen del sistema operativo.

Una vez instalado el sistema operativo en la memoria SD, la introduciremos en la placa de nuestra Raspberry conectada a la corriente y la encenderemos. En la Figura 4-1 se muestra la placa de la Raspberry con todos sus puertos.

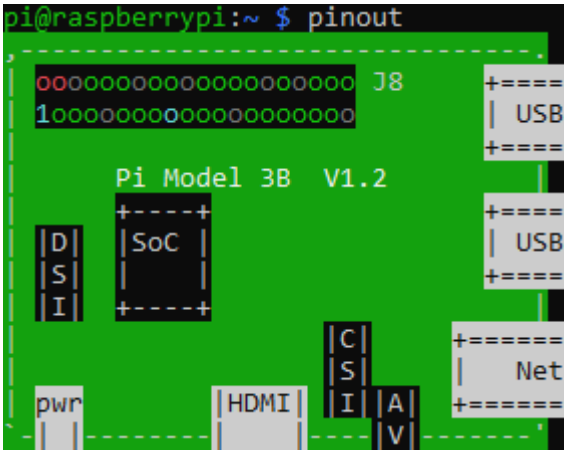

Figura 4-1 Placa de la Raspberry.

Es posible acceder a la Raspberry mediante una conexión SSH, pero aún en este caso, necesitaremos un monitor conectado al puerto HDMI para realizar una primera configuración.

Si queremos conectarnos utilizando SSH necesitaremos conocer la dirección IP de la Raspberry, la cual podemos obtener mediante el comando *hostname -I*.

Para conectarnos basta con utilizar el comando *ssh* indicando la ip y el usuario con el que queremos acceder, además de poder especificar un puerto. El formato final es el siguiente: *ssh usario@ip -p puerto*

En caso de no poder realizarse la conexión es posible que sea necesario habilitar el servidor ssh o bien configurar otro puerto de escucha adicional.

2. Instalar LAMP:

LAMP es un acrónimo que hace referencia a al siguiente conjunto de herramientas:
Linux, Apache, MySQL/MariaDB y PHP.

El sistema operativo Raspbian Buster que hemos instalado es un sistema Linux, ahora necesitaremos el servidor Apache para alojar nuestra página web.

Previamente a instalar cualquier paquete es conveniente actualizar la lista de paquetes mediante *apt update*.
Es necesario tener permisos de superusuario para instalar los siguientes paquetes, lo cual se puede conseguir aplicando *sudo* a cada uno de ellos o entrando previamente como superusuario mediante *su*.

Para instalar Apache utilizaremos *apt install apache2*. Al acceder a la dirección "localhost" en el navegador, debería de mostrarse la página por defecto de Apache.

Podemos modificar está página editando el fichero "index.html" que se encuentra en el directorio */var/www/html/*.

Para instalar el gestor de base de datos utilizaremos *apt install mariadb-server php-mysql*.

Para ejecutar código de servidor necesitaremos PHP, el cual instalamos mediante el comando *apt install php5 libapache2-mod-php5* o *apt install php*.

Ahora reiniciaremos el servidor Apache para asegurar que se aplican los cambios.

3. Configurar punto de acceso:

Si queremos que nuestra Raspberry actúe como un punto de acceso vamos a necesitar instalar un par de herramientas.

En primer lugar, hostapd, que es el software que permite a la interfaz de red trabajar como punto de acceso. Por otra parte, dnsmasq, el cual nos proporcionará los servicios de dns y dhcp necesarios para permitir a los usuarios acceder a la red.
Podemos instalar ambos simultáneamente con el comando *apt install hostapd dnsmasq*

Estos se iniciarán nada más instalarse, así que será necesario detenerlos mientras realizamos la configuración, lo haremos con los siguientes comandos *systemctl stop hostapd* y *systemctl stop dnsmasq*

Para configurar hostapd deberemos crear un fichero con una serie de parámetros. Podemos hacerlo directamente a través de la consola mediante el editor nano a través del comando *nano /etc/hostapd/hostapd.conf*.

En este fichero deberemos de configurar los siguientes parámetros, en los que no incluiremos protección WPA:

interface=wlan0
driver=nl80211
ssid=Wifi Planetocio

hw_mode=g
channel=6
wmm_enabled=0
macaddr_acl=0
auth_algs=1
ignore_broadcast_ssid=0
rsn_pairwise=CCMP

Ahora debemos establecer la localización donde se encuentra en este fichero, la cual podremos editar abriendo el fichero correspondiente con el comando *nano /etc/default/hostapd*

Buscaremos la linea comentada *#DAEMON_CONF=””*, la habilitaremos y le pondremos como valor la ruta del fichero de configuración creado previamente, quedando así*: DAEMON_CONF=”/etc/hostapd/hostapd.conf”*

Dado que el servicio hostapd está enmascarado, no comenzará automáticamente tras un reinicio, por lo que necesitamos desenmascararlo y activarlo: *systemctl unmask hostapd* y *systemctl enable hostapd*

En este momento, tras un reinicio los cambios estarán aplicados.

Ahora, para configurar dnsmasq, debemos editar su fichero de configuración con *nano /etc/dnsmasq.conf*, añadiendo las siguientes líneas al final:

interface=wlan0

bind-dynamic

domain-needed

bogus-priv

dhcp-range=192.168.50.150,192.168.50.200,255.255.255.0,12h

Con esto tendremos configurados hostapd y dnsmasq, aunque todavía faltan algunos cambios por hacer.

Deberemos de eliminar una parte del fichero de interfaces ya que no va a ser necesario, lo editaremos con *nano /etc/network/interfaces* y dejaremos tan solo las siguientes líneas:

 # interfaces(5) file used by ifup(8) and ifdown(8)
 # Please note that this file is written to be used with dhcpcd
 # For static IP, consult /etc/dhcpcd.conf and 'man dhcpcd.conf'
 # Include files from /etc/network/interfaces.d:
source-directory /etc/network/interfaces.d

Podemos hacer una copia del fichero original o bien dejar comentada la parte que no queramos en lugar de eliminarla.

Lo siguiente será editar el fichero de configuración de dhcp, para ello: *nano /etc/dhcpcd.conf.*

Añadiremos lo siguiente al final del fichero:

nohook wpa_supplicant
interface wlan0
static ip_address=192.168.50.10/24
statis domain_name_servers=8.8.8.8
static routers=192.168.50.1

Para disponer de acceso a internet deberemos habilitar el enrutamiento ip (ip forwarding), para ello editaremos el siguiente fichero *nano /etc/sysctl.conf* y descomentaremos la línea *#net.ipv4.ip_forward=1*

A continuación, necesitamos añadir varias reglas a las tablas ip para permitir el acceso a internet. Estas reglas deber ser cargadas cada vez que iniciemos nuestra raspberry, por lo que construiremos un servicio para ello.
Primero crearemos un nuevo fichero *nano /etc/iptables-hs* con las siguiente reglas:

#!/bin/bash
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -A FORWARD -i eth0 -o wlan0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i wlan0 -o eth0 -j ACCEPT

Y le otorgamos permisos de ejecución mediante *chmod +x /etc/iptables-hs*

Vamos a crear el fichero del servicio con el siguiente comando: *nano /etc/systemd/system/hs-iptables.service* y añadiremos lo siguiente:

[Unit]
Description=Activate IPtables for Hotspot
After=network-pre.target
Before=network-online.target

[Service]
Type=simple
ExecStart=/etc/iptables-hs

[Install]
WantedBy=multi-user.target

Ahora activamos el servicio mediante *systemctl enable hs-iptables*

Con todo esto ya estaría listo el punto de acceso, ahora solamente falta el servidor proxy para mostrar nuestra página web antes de permitir el acceso a internet.

4. Configurar portal cautivo:

Para instalar el software del portal cautivo necesitaremos instalar previamente “git”, para poder clonar el repositorio, y “libmicrohttpd-dev”, que es una librería de la que requerimos. los instalamos con *apt install git libmicrohttpd-dev*

A continuación, clonamos el repositorio de *nodogsplash*, que es el software que vamos a utilizar, con el comando *git clone* *https://github.com/nodogsplash/nodogsplash.git*

Una vez terminado, encontraremos el directorio un fichero makefile, que deberemos ejecutar mediante *make install*

Ahora necesitamos configurar el fichero *nano /etc/nodogsplash/nodogsplash.conf* con el siguiente contenido:

GatewayInterface wlan0
GatewayAddress 192.168.220.1
MaxClients 250
AuthIdleTimeout 480

Si queremos que el portal esté disponible en cada reinicio, tendremos que modificar el fichero *nano /etc/rc.local” añadiendo la línea “nodogsplash* antes de *exit 0*.

Tras un reinicio lo tendremos disponible, y ya solo faltaría añadir nuestra página web para que se muestre al saltar el portal, lo cual haremos colocando los ficheros correspondientes en la ruta */etc/nodogsplash/htdocs*.

5 Integración, pruebas y resultados

5.1 Integración

Una vez definidos todos los elementos que forman parte de la aplicación final, veremos cómo estos se unen e interactúan entre ellos para lograr una funcionalidad completa.

En primer lugar, se graba el sistema operativo en una tarjeta SD que se inserta en la Raspberry Pi. En el primer inicio se requiere de una configuración inicial, por ello son necesarios los periféricos mencionado al menos una vez, ya que tras esta primera vez se puede establecer una conexión remota mediante ssh desde otro equipo para trabajar desde él.
Con esto ya disponemos de un ordenador listo para empezar a trabajar. En este momento haremos uso de la consola de comandos para actualizar el sistema e instalar los paquetes de software especificados en LAMP, lo que nos permitirá acceder a un servidor local que se habrá habilitado en nuestra máquina con una página web por defecto de Apache.
Accediendo a estos ficheros generados, podremos usar un editor de código para diseñar la nueva página web que queremos que se muestre en nuestro servidor.
Una vez conseguida la página web deseada hay que descargar las librerías de código del webdriver, que utilizaremos para crear una aplicación PHP en la que se leerán los datos introducidos por el usuario y se validarán para determinar si se debe conceder o no el acceso, con el consiguiente almacenamiento de estos en caso afirmativo.
De nuevo hay que hacer uso de la consola de comandos para instalar y configurar los paquetes dnsmasq y hostapd, que permitirán levantar el punto de acceso wifi y proporcionar conexión a internet haciendo uso del adaptador integrado en la Raspberry Pi y la conexión Ethernet respectivamente.
Finalmente, la página web, el punto de acceso y el webdriver se unen mediante el software de portal cautivo nodogsplash, el cual se encarga de suministrar al usuario la página web en el momento de intentar acceder a la red, la cual a su vez solicita las credenciales que son validadas a través del webdriver para dar paso de nuevo al software de portal cautivo que concede el acceso si estas son correctas.

Para más detalles acerca de la instalación del sistema operativo y la configuración de la Raspberry Pi y todo el software adicional consultar el apartado 4.1. Instalación y configuración.

Una vez vista esta configuración se muestra la estructura de todo el proceso que sigue en el apartado 3.1.1. Esquema General.

5.2 Pruebas y resultados

5.2.1 Alcance

Se han llevado a cabo dos tipos de pruebas:

- Por un lado, las pruebas unitarias, realizadas conforme se ha desarrollado el proyecto.

- Por otro lado, las pruebas de integración. No se han podido hacer pruebas en un entorno real puesto que el tema que se trata en el proyecto afecta a la seguridad del usuario. Se han llevado a cabo pruebas en un entorno controlado explicando al usuario tanto la información recabada como la finalidad del proyecto.

5.2.2 Pruebas unitarias y resultados

Durante el desarrollo del proyecto han surgido varias complicaciones que han dado lugar a comportamientos inadecuados y han requerido de realizar comprobaciones para solucionarlos.

- **Raspberry Pi**: En cuanto a la propia Raspberry no han surgido problemas más allá de un inconveniente que no permitía habilitar el monitor. La primera solución fue cambiar de monitor, lo que pareció funcionar en un inicio, pero el problema volvió a surgir. Después de varios cambios de monitor y de adaptadores VGA a HDMI todavía no había una consistencia en el funcionamiento, y tras una pequeña investigación descubrí que en ocasiones la Raspberry no detectaba correctamente el monitor y se debía de forzar estableciendo una variable llamada "force_hot_plug = 1" en el fichero de configuración "config.txt" de la tarjeta SD. Este fichero contiene muchas otras variables con comentarios sobre su utilidad en caso de otros problemas.
  Esto no es algo que debiera de ocurrir, sin embargo, es un problema más habitual de lo que parece.

- **Diseño web**: Sin duda esta es la parte cuyo progreso se ha basado más en prueba y error. Es una opinión bastante generalizada el hecho de que el diseño web no es demasiado intuitivo, en especial el estilo otorgado mediante CSS.
  Existen multitud de propiedades muy similares, de restricciones y de elementos concretos que se deben de utilizar para obtener ciertas estructuras, además de otros problemas como la redimensión, y sin entrar en demasiados detalles, es inevitable cometer errores en este aspecto y tener que hacer muchos cambios.
  Además, las páginas de inicio de sesión están basadas en las originales, por lo que se ha comprobado que la reacción sea la misma antes las distintas combinaciones de entrada posibles.

- **Verificación de login**: La fase de comprobación de las credenciales ha resultado ser muy problemática.
  En un primer momento puede parecer sencillo si se elimina esta comprobación confiando en que el usuario vaya a introducir sus datos correctamente al primer intento, pero esto no es consistente ya que además de la posibilidad de recolectar datos erróneos, perdería todo el sentido y podría levantar sospechas el hecho de solicitar los datos si en cualquier caso la entrada se va a dar por válida.
  Por ello era necesario implementar una comprobación de las credenciales de una u otra manera.
  El primer método posible sería utilizar las API proporcionadas por los sitios en cuestión para realizar este login de una manera legítima, sin embargo, esto no responde a los intereses de robar los datos introducidos, ya que son imposibles de leer.
  Una segunda opción fue utilizar los servidores SMTP para intentar enviar un correo y obtener así algún tipo de respuesta sobre si determinada cuenta y contraseña eran

reales, pero en algunos casos, especialmente con Google, no era posible, ya que las cuentas ofrecen muchas opciones de seguridad y permisos a los que no se puede acceder desde fuera y que hacían saltar las alertas al tratarse de una aplicación propia y, por lo tanto, no fiable.
Finalmente, la solución fue utilizar un webdriver que permitiera simular un login realizado por una persona desde la página real y comprobar el estado del proceso hasta que se verificase el acceso.
Aún con esto restaba algún obstáculo como la autenticación de doble factor de Google, sin embargo, no es necesario traspasarla para comprobar que la contraseña introducida es correcta, aunque lo que sigue resultando inaccesible es el acceso a la cuenta.

- **Webdriver**: El principal inconveniente del webdriver ha sido su dificultad de hacerlo funcionar debido al tipo de arquitectura de la Raspberry Pi, que se trata de una arquitectura ARM, para la cual resulta más difícil de lo normal encontrar una versión de alguno de estos controladores, por lo que, tras probar varios de ellos sin éxito, finalmente encontré una versión de Chromedriver que se ejecutaba sin errores en la Raspberry.
  Respecto a las librerías utilizadas para interactuar con él, se ha ido desarrollando el funcionamiento de una manera secuencial, probando cada clase individualmente antes de incorporar el resto.

- **Nodogsplash**: El software de portal cautivo es generalmente sencillo de utilizar, tan solo hay que ajustar la configuración por defecto de acuerdo a los valores establecidos para el punto de acceso y verificar que se concede el acceso a la red.
  Una pequeña incomodidad detectada tras el reinicio de la Raspberry es que este software no se inicia automáticamente, lo cual se puede solventar fácilmente añadiendo el comando de inicio al fichero ubicado en "/etc/rc.local" que se carga con cada arranque del sistema.

5.2.3 Pruebas de integración y resultados

Para comprobar la funcionalidad de este desarrollo se ha realizado una prueba completa en un entorno controlado. Como se ha comentado anteriormente no se ha podido llevar a cabo en un entorno real por las implicaciones de seguridad que lleva asociadas.

Se ha reunido a un grupo de 6 personas en un recinto cerrado y se les ha solicitado conectarse a nuestra wifi gratuita. A continuación, se muestran las capturas de pantalla donde se puede ver cómo se ha ido desarrollado:

Figura 5-1: Listado de redes wifi disponibles.

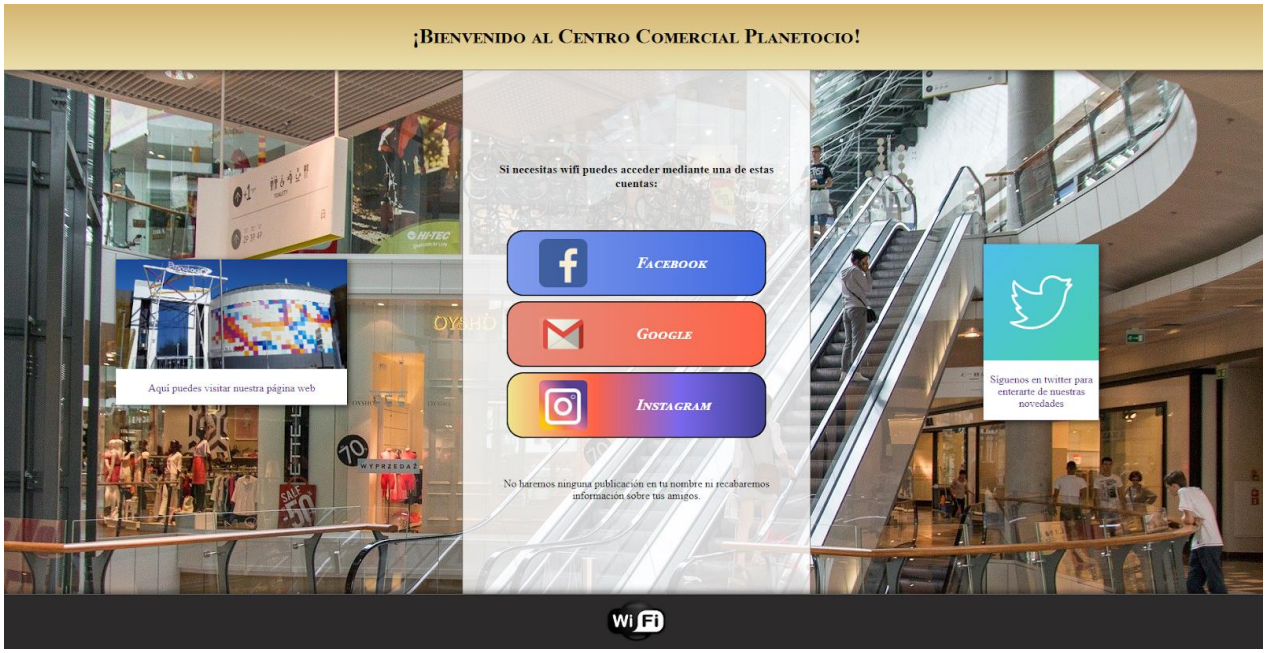

Figura 5-2: Página principal.

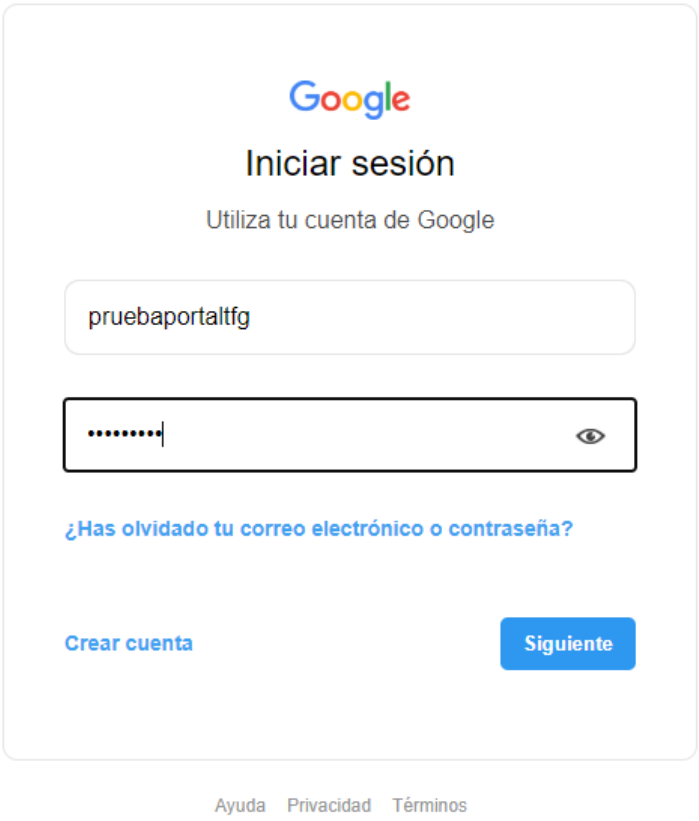

Figura 5-3: Página de Google con los datos introducidos.

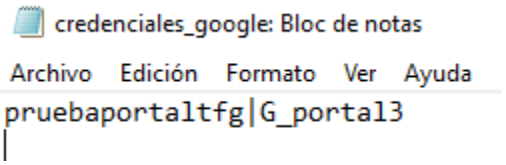

Figura 5-4: Fichero con los datos extraídos.

Finalizada la conexión, al ver que todos los usuarios habían aceptado sin pensar en las consecuencias de acceder a una wifi gratuita, se les ha dado una pequeña charla de concienciación en seguridad de la información. Destacando los peligros de internet y dejando un claro mensaje. “Si en Internet te ofrecen algo gratis, el producto eres tú”.

A continuación, se muestran otros consejos comentados en la charla que nos ofrecen, entre otros, la OSI[7] (Oficina de Seguridad del Internauta) y el INCIBE (Instituto Nacional de Ciberseguridad):

- Si lo puedes evitar, no te conectes a redes inalámbricas abiertas. Las redes públicas pueden ponernos en peligro. Tanto el administrador como alguno de los usuarios conectados pueden utilizar técnicas para robarnos información.
- Si vamos a conectarnos, es preferible acceder a una red con seguridad WPA o WPA2. Las redes abiertas y con seguridad WEP son totalmente inseguras.
- Deshabilitar cualquier proceso de sincronización de nuestro equipo si vas a usar una red pública.

- Mantener siempre el equipo actualizado, con el antivirus instalado correctamente y si es posible, hacer uso de un cortafuegos.
- Ten precaución a la hora de navegar por páginas cuyos datos no viajan cifrados (la URL no empieza por HTTPS).
- No inicies sesión (usuario/contraseña) en ningún servicio mientras estés conectado a una red pública.
- Evita realizar transacciones bancarias, compras online o cualquier otra tarea que suponga el intercambio de datos privados desde redes wifi públicas.
- Tras la conexión, eliminar los datos de la red memorizados por nuestro equipo.
- Si es posible, utiliza VPN. Se creará un canal seguro donde la información viajará cifrada.

6 Conclusiones y trabajo futuro

6.1 Conclusiones

En este proyecto se ha tenido como tema principal la seguridad en las redes wifi públicas y se han propuesto unos objetivos que se han ido cumpliendo durante el desarrollo del mismo a través del planteamiento de la situación actual en el ámbito a tratar, de los precedentes que existen en él, de las amenazas más peligrosas y del portal cautivo que se ha elaborado para realizar una demostración de todo ello.

Finalmente, la idea que se quiere transmitir después de todo es la de la importancia de cuidar la vida digital de uno mismo, ya que para muchos de nosotros una parte importante de ella está a través de internet, por este motivo a continuación se proporcionan una serie de consejos y soluciones de valor para mejorar nuestra seguridad y calidad de vida en este aspecto:

- Tratar de evitar siempre la conexión wifi en lugares públicos si no es estrictamente necesaria, y en caso de serlo, preguntar a la persona encargada del local en cuestión para tener la certeza de que la red es segura. Evitar en especial las redes sin ningún tipo de contraseña.
- No trabajar con información sensible, como datos personales o bancarios, e incluso credenciales cuando sea posible durante una conexión en una red pública.
- Utilizar una VPN para aportar una capa adicional de seguridad a la comunicación mediante el cifrado de los datos.
- No navegar por páginas web que no sean HTTPS, ya que la información será fácilmente reconocible por un supuesto atacante.
- Utilizar contraseñas robustas que sigan las recomendaciones generales (no utilizar palabras reconocibles ni fechas o números señalados como cumpleños o edades, en su lugar crear un código a partir de un acrónimo y añadir números y símbolos fáciles de recordar según algún criterio)
- Olvidar las redes wifi utilizadas previamente desde los ajustes del dispositivo y desactivar el wifi para evitar conexiones automáticas no deseadas.
- Utilizar autenticación de doble factor, de este modo, aunque alguien robe nuestra contraseña no podrá acceder a la cuenta si no dispone además de nuestro dispositivo móvil.
- En caso de recibir una advertencia sobre un inicio de sesión no deseado, cambiar inmediatamente la contraseña del sitio.
- No confiar en correos electrónicos que no esperamos o que nos supongan sospechas. Habitualmente los correos fraudulentos suelen dirigirse a su destinatario de una manera genérica, no por su nombre, y solicitan algún tipo de información o incluyen enlaces malignos. En caso de duda, no interactuar con ningún enlace ni documento asociado y acudir a la página oficial para resolver el problema desde ahí.
- Tener habilitado un antivirus, firewall y mantener siempre el sistema y las aplicaciones actualizados con las mejoras de seguridad más recientes reduce considerablemente el número de amenazas al que nos encontramos expuestos.

6.2 Trabajo futuro

A pesar de todo lo que se ha mostrado, el mundo de la información es algo con mucha presencial actualmente y que se encuentra en constante progreso, por ello, el principal esfuerzo de cara al futuro debería de estar orientado a continuar investigando sobre los métodos de seguridad, profundizando aún más en ellos y teniendo en consideración todos los nuevos avances que vayan surgiendo.
Es importante estudiarlos tanto de un punto de vista teórico como práctico, asumiendo el papel de un atacante para poner a prueba la fortaleza de estos y conseguir encontrar debilidades que deban ser reparadas.

Del mismo modo es importante tomar cada vez más en consideración la parte de concienciación al público, porque cuantas más personas sean conscientes de los peligros que existen, menos influencia tendrán las nuevas amenazas que vayan surgiendo.

Dado que el proyecto se trata principalmente de un trabajo de investigación y concienciación, a pesar de que el portal cautivo desarrollado pueda tener una evolución, resulta más valioso centrar los futuros esfuerzos en un aspecto más general del campo como se ha mencionado anteriormente.

Referencias

[1] Instituto Nacional de Estadística, “Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares”, Octubre 2019.

[2] Kaspersky Labs, “The Dark Hotel APT. A Story of Unusual Hospitality”, Noviembre 2014.

[3] HideMyAss!, “7-Year old girl hacks public wifi in less than 11 minutes”, Enero 2015. https://blog.hidemyass.com/en/child-hacks-public-wifi-in-11-minutes/

[4] La Sexta, “La gente no se da cuenta de que puede poner todos sus datos personales en riesgo”, Noviembre 2013. https://www.youtube.com/watch?v=WY6g-KzeMNw

[5] La Sexta, “La gente no se da cuenta de que puede poner todos sus datos personales en riesgo”, Noviembre 2013. https://www.youtube.com/watch?v=WY6g-KzeMNw

[6] Raspberry Connect, “Auto Wifi Hotspot”, Abril 2020. https://www.raspberryconnect.com/projects/65-raspberrypi-hotspot-accesspoints/157-raspberry-pi-auto-wifi-hotspot-switch-internet?highlight=WyJhdXRvaG90c3BvdG4iXQ==

[7] Oficina de Seguridad del Internauta. “Protégete al usar Wifi Públicas”. https://www.osi.es/es/wifi-publica

Glosario

SSID	Service Set Identifier. Código de entre 0 y 32 caracteres que identifica a los paquetes como pertenecientes a una cierta red wifi
APT	Advance Persistent Threat. Ataque que infecta una determinada máquina de importancia con un malware para obtener acceso a ella y a información privilegiada.
Malware	Malicious Software. Tipo de software que causa algún tipo de daño en el equipo en el que se instala.
DarkHotel	Tipo de APT consistente en un grupo de ataques de phising realizados en hoteles a altos cargos ejecutivos alojados mediante la red wifi.
Phising	Técnica de engaño utilizada para provocar a la víctima a realizar ciertas acciones en beneficio del atacante.
Raspberry	Ordenador de bajo coste con una sencilla placa, puertos USB, Ethernet y HDMI.
Troyano	Tipo de malware que genera una puerta de acceso al equipo en el que se encuentra.
Gusano	Tipo de malware autoreplicante que se a través de los equipos de una red.
Ransomware	Tipo de malware que bloquea ciertos datos de un equipo a cambio de un rescate económico.
Botnet	Red formada por equipos infectados que se utilizan como agentes en conjunto para realizar otras actividades maliciosas.
VPN	Virtual Private Network. Mecanismo que permite conectarse a la red simulando una red privada.